Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A method for booting up a computer system in a secure fashion comprising [the steps of]:

a) determining the presence of a security feature element during an initialization of the computer system, wherein the security feature element is installed within a housing of the computer system such that a cover to the housing is opened to remove the security feature element, and wherein the security feature element stores [includes] a public key and a corresponding private key;

b) storing a portion of the public key from the security feature element in a nonvolatile memory within the computer system if the security feature element is present; and

c) utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system, wherein additional authorization is required to be input to the computer system to boot up the computer system if the security feature element is not present and was previously present in the computer system.

2. (original) The method of claim 1 wherein the security feature element comprises a security card.

3. (original) The method of claim 2 wherein the security card provides for tamper detection of the computer system and the security card, temperature monitoring of the computer system and voltage status reporting of the computer system.

4. (original) The method of claim 1 wherein step c) is performed during a Power-On-Self-Test (POST) sequence.

5. (currently amended) The method of claim 4 wherein step c) further comprises:

c1) determining the presence of the security [card] feature element.

6. (currently amended) The method of claim 5 wherein step c1) further comprises:

c1a) determining if the computer system has been subjected to a tamper event if the security [card] feature element is present.

7. (currently amended) The method of claim [6] 5 wherein step c1) further comprises:

c1a) determining whether a security [card] feature element was previously present in the computer system if the security [card] feature element is not present.

8. (currently amended) The method of claim 7 wherein step c1) further comprises:

c1b) clearing the portion of the public key stored in the non-volatile memory of the computer system if a security [card] feature element was previously present in the computer system; and

c1c) prompting for an authorization prior to booting up the computer system.

9. (currently amended) The method of claim 7 wherein step c1) further comprises:

c1b) booting up the computer system if the security [card] feature element was not previously present in the computer system.

10. (original) The method of claim 6 wherein step c1) further comprises:

c1b) booting up the computer system if the computer system has not been subjected to a tamper event.

11. (currently amended) The method of claim 6 wherein step c1) further comprises:

c1b) determining whether the security [card] feature element is an added feature of the computer system, wherein the determination is based on a previous POST sequence, if the computer system has been subjected to a tamper event.

12. (currently amended) The method of claim 11 wherein step c1) further comprises:

c1c) clearing the portion of the public key stored in the nonvolatile memory of the computer system from previously-installed security feature elements if the [card] security feature element is a newly added feature of the computer system; and

c1d) prompting for an authorization prior to booting up the computer system.

13. (currently amended) The method of claim 11 wherein step c1) further comprises:

c1c) comparing the public key on the security [card] feature element with the

portion of the public key stored in the nonvolatile memory of the computer system if the security [card] feature element is not a newly added feature of the computer system.

14. (currently amended) The method of claim 13 wherein step c1) further comprises:

c1d) booting up the computer system if the public key on the security [card] feature element matches the portion of the public key stored in the nonvolatile memory of the computer system.

15. (currently amended) The method of claim 13 wherein, if the public key on the security feature element does not match the portion of the public key stored in the nonvolatile memory of the computer system, step c1) further comprises:

c1d) clearing the portion of the public key stored in the nonvolatile memory of the computer system;

c1e) clearing the public key and the corresponding private key stored on the security [card] feature element; and

c1f) [booting up the computer system] prompting for an authorization prior to booting up the computer system.

16. (currently amended) A system for booting up a computer in a secure fashion, the system comprising:

means for determining the presence of a security feature element during an initialization of the computer system, wherein the security feature element is installed within a housing of the computer system such that a cover to the housing is opened to remove the

security feature element, and wherein the security feature element stores [includes] a public key and a corresponding private key;

means for storing a portion of the public key from the security feature element in a nonvolatile memory within the computer system if the security feature element is present; and

means for utilizing an algorithm to determine the presence of the security feature element prior to a subsequent boot-up of the computer system, wherein additional authorization is required to be input to the computer system to boot up the computer system if the security feature element is not present and was previously present in the computer system.

17. (original) The system of claim 16 wherein the security feature element comprises a security card.

18. (original) The system of claim 17 wherein the security card provides for tamper detection of the computer and the security card, temperature monitoring of the computer and voltage status reporting of the computer.

19. (original) The system of claim 18 wherein the algorithm is utilized during a Power-On-Self-Test (POST) sequence.

20. (original) The system of claim 19 wherein the means for utilizing the algorithm further comprises:

means for determining the presence of the security card.

21. (original) The system of claim 20 wherein the means for utilizing the algorithm further comprises:

means for determining if the computer has been subjected to a tamper event if the security card is present.

22. (original) The system of claim 20 wherein means for utilizing the algorithm further comprises:

means for determining whether a security card was previously present in the computer if the security card is not present.

23. (original) The system of claim 22 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the non-volatile memory of the computer if a security card was previously present in the computer; and

means for prompting for an authorization prior to booting up the computer.

24. (original) The system of claim 22 wherein the means for determining the presence of the security card further comprises:

means for booting up the security system if the security card was not previously present in the computer.

25. (original) The system of claim 21 wherein the means for determining the presence of the security card further comprises:

means for booting up the computer if the computer has not been subjected to a tamper event.

26. (original) The system of claim 21 wherein the means for determining the presence of the security card further comprises:

means for determining whether the card is a newly added feature of the computer, wherein the determination is based on a previous POST sequence, if the computer has been subjected to a tamper event.

27. (currently amended) The system of claim 26 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the nonvolatile memory of the computer from previously-installed security feature elements if the card is a newly added feature of the computer; and

means for prompting for an authorization prior to booting up the computer.

28. (original) The system of claim 26 wherein the means for determining the presence of the security card further comprises:

means for comparing the public key on the security card with the portion of public key stored in the nonvolatile memory of the computer if the security card is not a newly added feature of the computer.

29. (original) The system of claim 28 wherein the means for determining the presence of the security card further comprises:

means for booting up the computer system if the public key on the security card matches the portion of the public key stored in the nonvolatile memory of the computer.

30. (currently amended) The system of claim 28 wherein the means for determining the presence of the security card further comprises:

means for clearing the portion of the public key stored in the nonvolatile memory of the computer, and for clearing the public key and the corresponding private key stored on the security card, if the public key on the security feature element does not match the portion of the public key stored in the nonvolatile memory of the computer system;

~~means for clearing the public key and the corresponding private key stored on the security card;~~ and

means for prompting for an authorization prior to booting up the computer if the public keys stored in the nonvolatile memory and the security feature element are cleared.

31. (new) The method of claim 1 wherein the security feature element comprises a security card installed in a slot of a system board in the computer system.

32. (new) The method of claim 6 wherein the tamper event includes the cover of the housing of the computer system having been opened.

33. (new) The system of claim 16 wherein the security feature element comprises a security card installed in a slot of a system board in the computer system.

34. (new) The system of claim 21 wherein the tamper event includes the cover of the housing of the computer system having been opened.

35. (new) A method for booting up a computer system in a secure fashion comprising:

a) determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key;

b) storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present; and

c) upon, and prior to, a subsequent boot-up of the computer system,

1) determining the presence of the security feature element;

2) determining whether the computer system and security feature element have been subjected to a tamper event if the security feature element is present;

3) determining whether the same security feature element was present previously in the computer system; and

4) allowing the computer system to be booted up if the security feature element is present, if the computer system has been subjected to a tamper event, and if the same security feature element is determined to have been previously present.

36. (new) The method of claim 35 wherein the same security feature element is determined to have been previously present by checking whether the public key of the security feature matches the stored portion of the public key in the nonvolatile memory within the computer system.

37. (new) The method of claim 36 wherein the same security feature element is determined to have been previously present by determining whether the security feature element is an added feature of the computer system.

38. (new) The method of claim 37 wherein step c) is performed during a Power-On-Self-Test (POST) sequence, and wherein determining whether the security feature element is an added feature of the computer system includes checking a previous POST sequence.

39. (new) The method of claim 35 further comprising allowing the computer system to be booted up if the security feature element is present and if the computer system has not been subjected to a tamper event.

40. (new) The method of claim 35 further comprising determining whether a security feature element was previously present in the computer system if the security feature element is not present.

41. (new) The method of claim 40 wherein, if the security feature element is not present and if a security feature element was previously present in the computer system,

further comprising clearing the portion of the public key stored in the non-volatile memory of the computer system and prompting for an authorization prior to booting up the computer system.

42. (new) The method of claim 35 wherein step c) is performed during a Power-On-Self-Test (POST) sequence, and further comprising determining whether the security feature element is an added feature of the computer system if the computer system has been subjected to a tamper event, wherein the determination is based on a previous POST sequence.

43. (new) The method of claim 42 wherein, if the security feature element is a newly added feature of the computer system and if the computer system has been subjected to a tamper event, further comprising:

clearing the portion of the public key stored in the nonvolatile memory of the computer system; and

prompting for an authorization prior to booting up the computer system.

44. (new) The method of claim 35 wherein, if the public key on the security feature element does not match the portion of the public key stored in the nonvolatile memory of the computer system, further comprising:

clearing the portion of the public key stored in the nonvolatile memory of the computer system;

clearing the public key and the corresponding private key stored on the security

feature element; and

prompting for an authorization prior to booting up the computer system.

45. (new) The method of claim 35 wherein the security feature element comprises a security card installed in a slot of a system board in the computer system.

46. (new) The method of claim 35 wherein the security feature element is installed within a housing of the computer system such that a cover to the computer system must be opened to remove the security feature element.

47. (new) The method of claim 35 wherein a tamper event includes a cover to a housing of the computer system being opened.

48. (new) A method for booting up a computer system in a secure fashion comprising:

a) determining the presence of a security feature element during an initialization of the computer system wherein the security feature element includes a public key and a corresponding private key;

b) storing a portion of the public key in a nonvolatile memory within the computer system if the security feature element is present; and

c) utilizing an algorithm during a Power-On-Self-Test (POST) sequence of the computer system to:

1) determine the presence of the security feature element prior to a subsequent boot-

up of the computer system;

2) determine if the computer system has been subjected to a tamper event if the security card is present;

3) determine whether the security card is an added feature of the computer system, wherein the determination is based on a previous POST sequence, if the computer system has been subjected to a tamper event;

4) compare the public key on the security card with the portion of the public key stored in the nonvolatile memory of the computer system if the security card is not a newly added feature of the computer system; and

5) if the public key on the security card does not match the portion of the public key stored in the nonvolatile memory of the computer system,

i) clear the portion of the public key stored in the nonvolatile memory of the computer system;

ii) clear the public key and the corresponding private key stored on the security card; and

iii) boot up the computer system.

49. (new) The method of claim 48 wherein step c) further comprises clearing the portion of the public key stored in the nonvolatile memory of the computer system and prompting for an authorization prior to booting up the computer system, if the security feature element is a newly added feature of the computer system.

50. (new) The method of claim 48 wherein step c) further comprises booting up the

computer system if the public key on the security feature element matches the portion of the public key stored in the nonvolatile memory of the computer system.

51. (new) The method of claim 48 wherein step c) further comprises booting up the computer system if the computer system has not been subjected to a tamper event.